Chapter 5
SECURITY

501 INTRODUCTION

In coalition and allied domains the challenge is to exchange releasable information freely between national, allied and coalition networks without compromising that information, despite the fact that these networks may be connected electronically if not logically. Undue restrictions on the flow of information from national domains to allied and coalition domains will adversely affect the quality and timeliness of that information. This would hamper the network member's ability to conduct effective and efficient operations.

502 AIM

The aim of this chapter is to provide information security requirements for the management of IP networking within a MNTG.

503 DEFINITIONS

The following definitions apply:

a. **Allied** — Two or more of the five CCEB nations operating together

b. **Coalition** — One of more of the five CCEB nations operating together with other nations (including NATO)

c. **Joint** — Two or more of the armed services from one nation operating together

d. **Combined** — Joint forces from two or more Allied nations operating together

504 NETWORK TOPOLOGY

a. For a network to provide efficient and effective allied/coalition C2, it is envisaged that secure RF bearers would connect a layered system of networks comprised of Allied, Coalition and National components. This is represented in Figure 5-1. Local area network(s) (LAN) located in national platforms and connected by RF bearers would in effect establish a MTWAN. A MTWAN will normally be connected to an Allied Wide Area Network (Allied WAN) to provide wider communications and may or may not be connected to a Coalition Wide Area Network (CWAN).

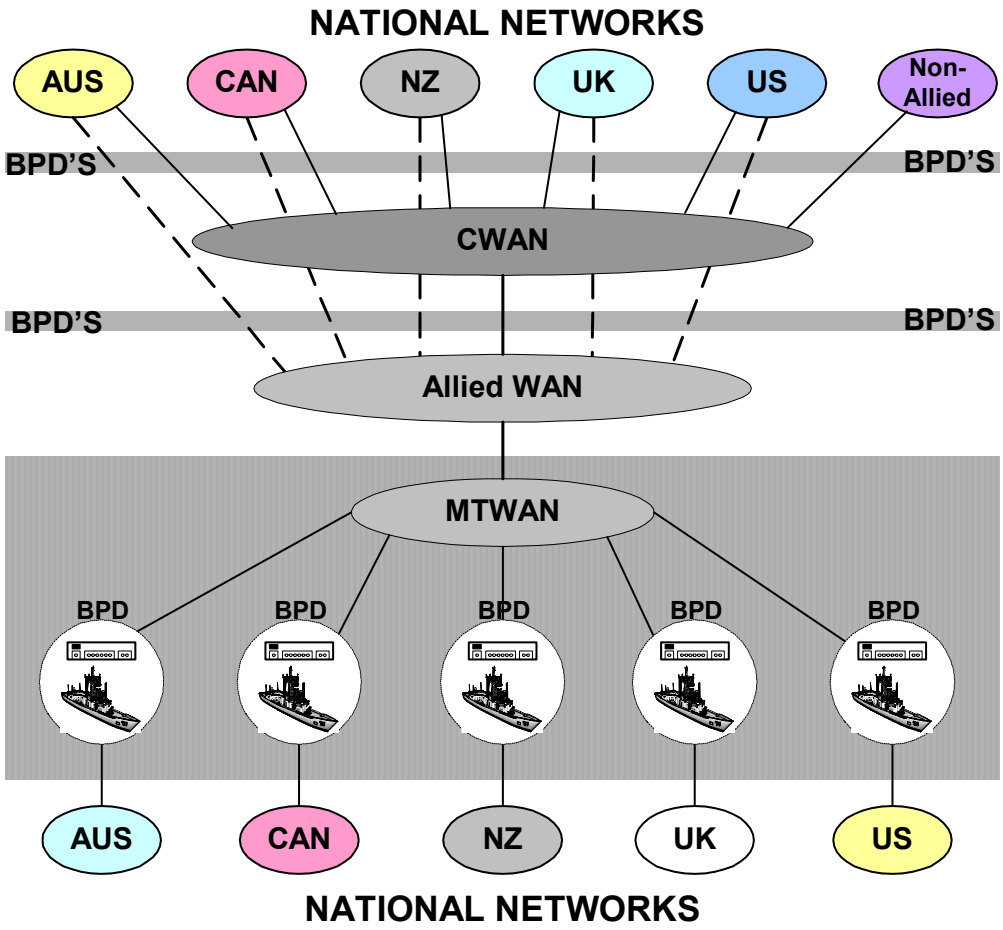

Figure 5-1: – MTWAN Topology

b. Within the boundaries of a MTWAN security domain, the network will not contain protection mechanisms, which unduly restrict the availability of information; a MTWAN and Allied WANs are regarded as peer-to-peer networks.

c. However, connection of a MTWAN or Allied WANs to either the National Networks and/or CWAN requires protection mechanism(s) to provide the appropriate degree of security for resources and information services contained in the National or CWAN sensitive domains. The protection mechanism(s) between a MTWAN and a National Network will be consistent with each nation's security policy. It will be such that neither Allied-only releasable information contained within a MTWAN/Allied WANs nor Coalition-only releasable information contained within the CWAN is compromised by unauthorised access.

d. The protection mechanism employed in a MTWAN topology is referred to as a Boundary Protection Device (BPD), also referred to as Point of

Presence (POP), this may either be an electronic device, a software suite contained in a component of the WAN or a person who performs this function. The BPD acts to prevent logical connections across domains by the use of a demilitarized zone (DMZ) between the two (Figure 5-2 refers), supported by procedures to ensure its correct operation.

e. It is recognized that the use of protection mechanisms will restrict the flow of information at the boundaries between a MTWAN/Allied WAN and National and Coalition domains, and the restrictions may affect the quality and timeliness of information moving between the domains. However, protection of sensitive information within these three distinct domains remains paramount.

505 RISK

Leakage of unauthorized information and penetration by unauthorized users are inherent risks in networks and may result in compromises to the confidentiality, integrity or availability of either the system or the information it contains. These risks are summarized below:

a. **Confidentiality**. Assurance that information is not disclosed to unauthorized persons, processes, or devices.

b. **Integrity**. Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.

c. **Availability**. Timely, reliable access to data and information services for authorized users.

d. **Accidental Leakage**. When information is released inadvertently by either the system itself or an operator contrary to the security regulations pertaining to that information. A risk exists if the outbound data is transferred unscreened or without label checks, either in real time or off line.

e. **Deliberate Leakage**. When information is released by an operator contrary to the security regulations pertaining to that information. A risk exists if the outbound data is transferred unscreened, either in real time or off line.

f. **Stimulated Leakage (Masquerade)**. When an attacker pretends to be someone else to stimulate the release of information contrary to the security regulations pertaining to that information.

g. **Stimulated Leakage (Trojan Horse)**. When malicious software stimulates the release of information contrary to the security regulations pertaining to that information.

h. **Corruption of Information (Malicious Code)**. When a harmful payload (virus, worm or Trojan Horse) is introduced into a system, either deliberately or inadvertently via the protocol being passed, which corrupts data contained within that system. A risk exists, however this risk can be reduced by the use of screening software and Intrusion Detection Systems.

i. **Denial of Service from Malicious Code**. When a harmful payload (virus, worm or Trojan Horse) is introduced into a system, either deliberately or inadvertently via the protocol being passed, which prevents the operation of applications or services within that system. A risk exists, however this risk can be reduced by the use of screening software and Intrusion Detection Systems.

j. **Denial of Service from Flooding**. When applications or services within a system are prevented from operating after its memory devices have been swamped by the introduction of large volumes of data via the inbound leg. A risk exists, however this risk can be reduced by the use of screening software and Intrusion Detection Systems.

k. **Spoofing (Masquerade)**. Where an attacker masquerades as someone else to distort the view of the reader about the incoming information.

506 RESPONSIBILITIES

a. Nations have a requirement to protect sensitive and national “eyes-only” information on national networks. The responsibility for the protection of this information resides with the individual nations. Nations will be responsible for ensuring that approved cryptographic devices and IA products (e.g. guards) are employed where required and that national COMSEC standards, including key management, are met at all times.

b. Any BPD placed between these national networks and a MTWAN will be nationally owned and controlled. However, the protection of information on a MTWAN itself is the responsibility of the Allied participants as a whole. Autonomous System(s) (AS) that leave a MTWAN remain responsible for the continued protection of data that had been externally provided to a MTWAN. This is of particular concern if the AS is to connect to a third party network.

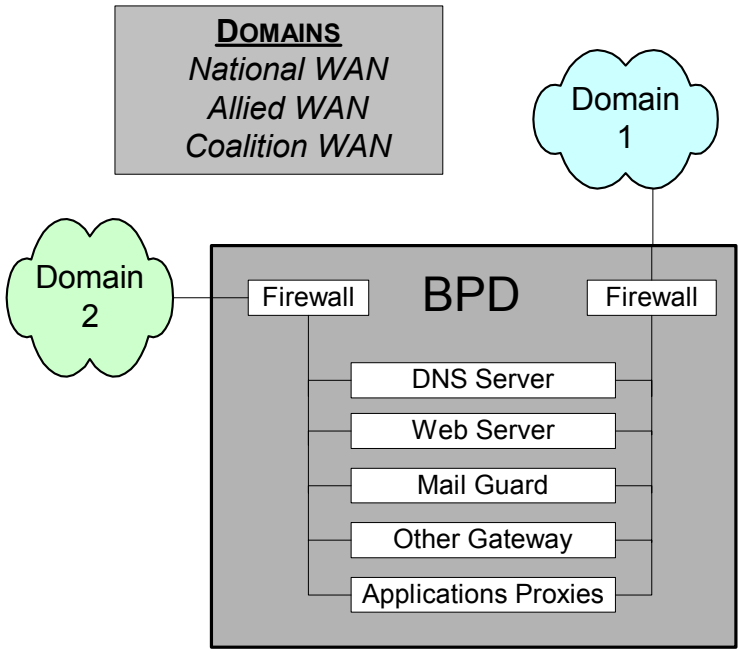

Figure 5-2: – Boundary protection devices between domains

507 PERMITTED INFORMATION FLOW ACROSS BPD

a. A MTWAN delivers a range of information services to mobile platforms in support of tactical naval operations. These services will include military messaging, the exchange of a Common Operational Picture (COP) and tailored tactical pictures, information pull, profile-based information push and Distributed Collaborative Planning (DCP), VTC and voice. BPDs between National, Allied and Coalition domains must therefore be capable of constraining the degree of interaction between the domains whilst permitting the following information flow characteristics:

(1) Bi-directional messaging with attachments;

(2) Export or publication of files, documents and database information; and

(3) Retrieval of information from either external systems within the domains themselves or shared export repositories normally positioned within the DMZ.

b. The BPD will require the following functionality:

(1) **Guard** - to control the release of information between National, Allied and Coalition networks; and

(2) **Firewall** - to protect the National, Allied and Coalition networks against unwanted intrusion.

c. The BPD will provide some or all of the following functions:

(1) packet-level filtering;

(2) address translation;

(3) port number filtering; and

(4) application proxying.

508 EXPORT SANCTION

It is envisaged that BPDs should be able to carry out Export Sanction to guard against accidental and stimulated leakage from the National domain. In addition, BPDs should provide audit and traceability capabilities to limit the attractiveness of deliberate leakage across the boundary. This function is mandatory in the BPD between a MTWAN/Allied WAN and the CWAN or any other Coalition network. Between a National domain and Allied or Coalition domains, this functionality is entirely the responsibility of the nation concerned.

509 ASSUMPTIONS

The following assumptions are made:

- Nations have agreed security principles and tenets.
- Nations have accepted information protection requirements and are working toward a yet to be determined commonality.
- A MTWAN will operate at the SECRET system high level with information releasable to all MTWAN participants.
- All personnel with access to a MTWAN will be cleared to the appropriate level.
- National networks will have been accredited through a mutually agreed process prior to any connection to a MTWAN.
- No connections to National networks will be permitted without passing through a BPD.
- All communications subnets will be protected by High Grade military crypto devices.
- Technical solutions for the BPD will not be required, to prevent intentional security breaches by cleared personnel. However, there is a requirement for the existence of some sort of audit or trace mechanism.
- Network nodes are to have appropriate physical, personnel and procedural security measures in place.

- Proposed architectural solutions will not mandate the use of specific applications or products on nations.
- COTS hardware and software will be used where ever possible.

510 RECOMMENDED SECURITY ARCHITECTURES

a. **Network Connectivity.** A MTWAN will be an AS connected to the Allied WAN through a Network Operations Center (NOC) as shown in Figure 5-3. There are three potential shipboard architectures that have the potential to meet the security requirements. Current technology does not permit the implementation of the integrated solutions; it is intended to migrate to these solutions as technology and policy allows.

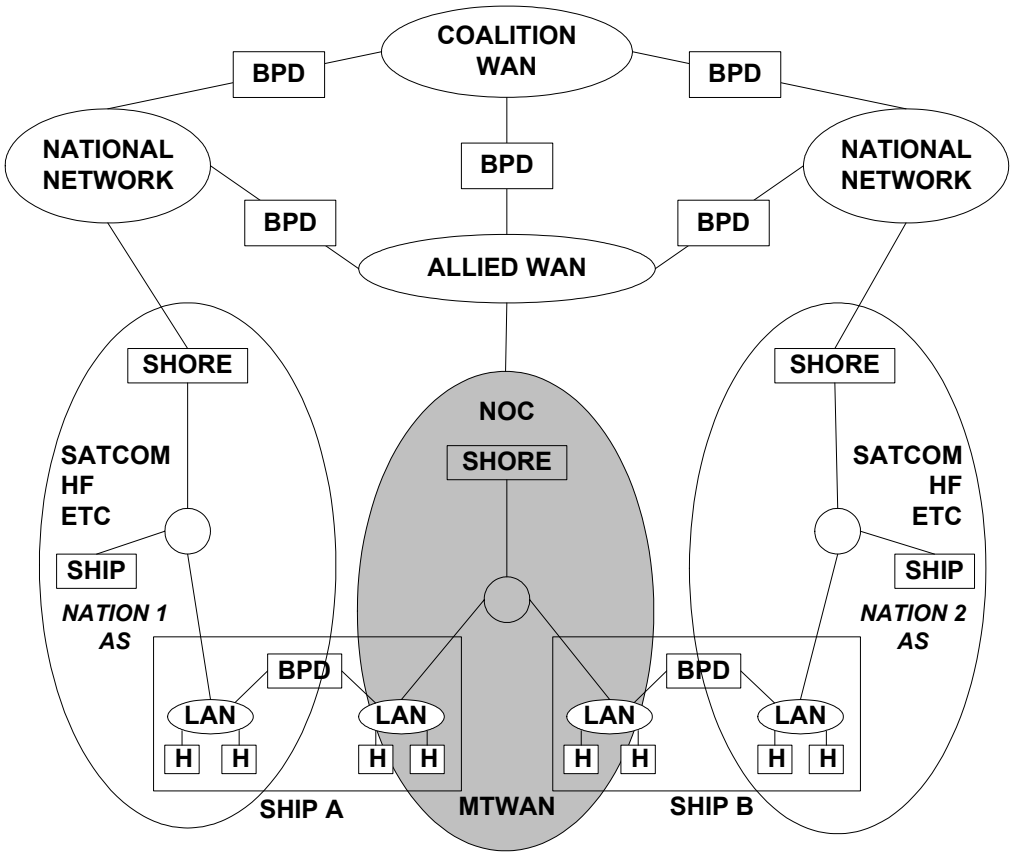

Figure 5-3: - MTWAN Connectivity

b. **Shipboard "Air Gap" Architecture.** An air gap between the National network and a MTWAN, as shown in Figure 5-4, provides information security for mobile platforms. This air gap architecture relies on physical access control — manual intervention is required to sanitise and transfer information between the two networks via magnetic media such as floppy disks, or keyboards. This is a short-term solution until a faster, efficient and secure process is developed and accredited.

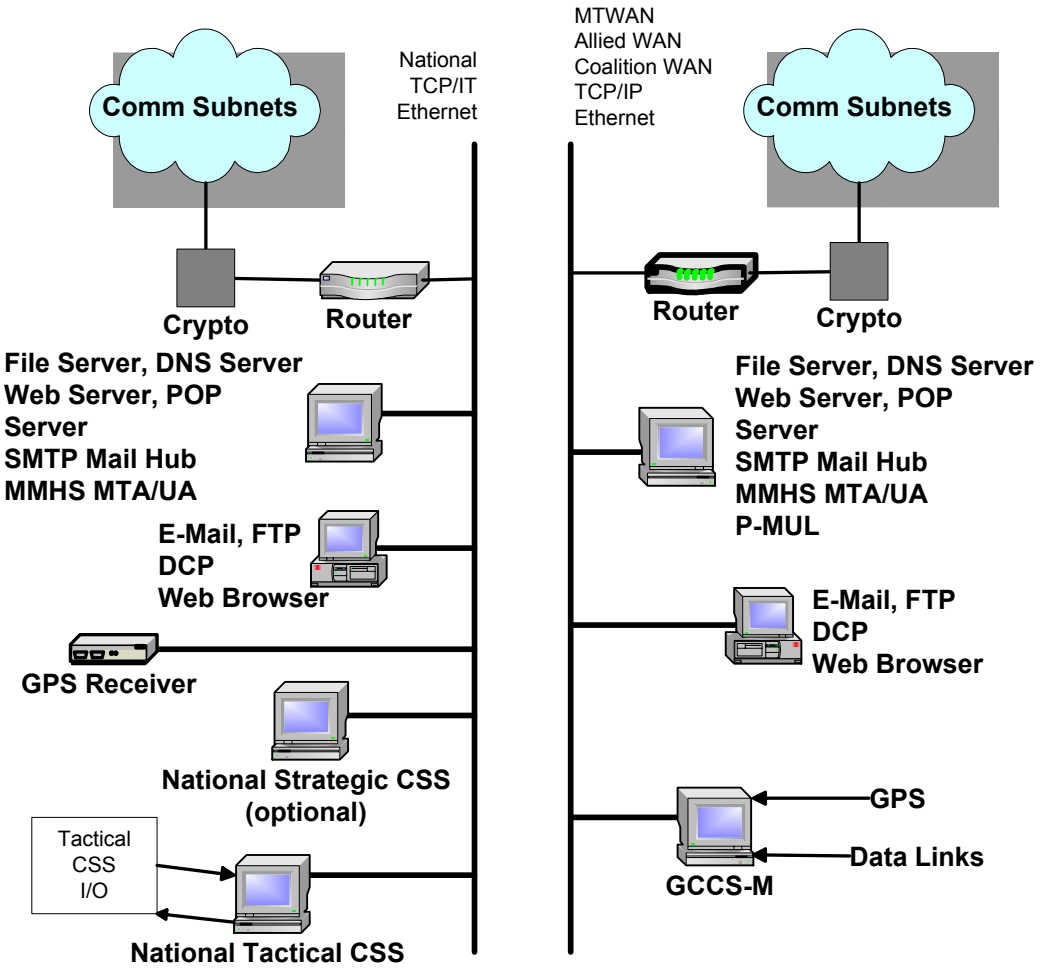

Figure 5-4: - Air Gap Architecture

c. **Shipboard "Networked" Architecture.** The ability to exchange information electronically will be required to support the increasing amount of information against the requirement for timely delivery. The architecture shown in Figure 5-5 supports electronic transfers between two networks. Information security will be achieved through a combination of physical, technical and procedural methods. Shipboard "Fully Integrated" Target Architecture. A result of the air-gap and networked solutions is the duplication of resources (e.g. multiple LANs and workstations). This imposes considerable penalties in terms of cost, space and weight. The preferred solution, therefore, is to provide access to both a MTWAN and National networks from a single on-board network.

d. By increasing the capability of the security gateway, the duplicate services supported on a MTWAN can be reduced and ultimately eliminated. This will depend on the availability of suitable application proxies and guards. For example, existing COTS/GOTS technology would allow screening

routers and bastion hosts to provide guards for e-mail; however, DCP will need to be supported by a workstation directly connected to a MTWAN.

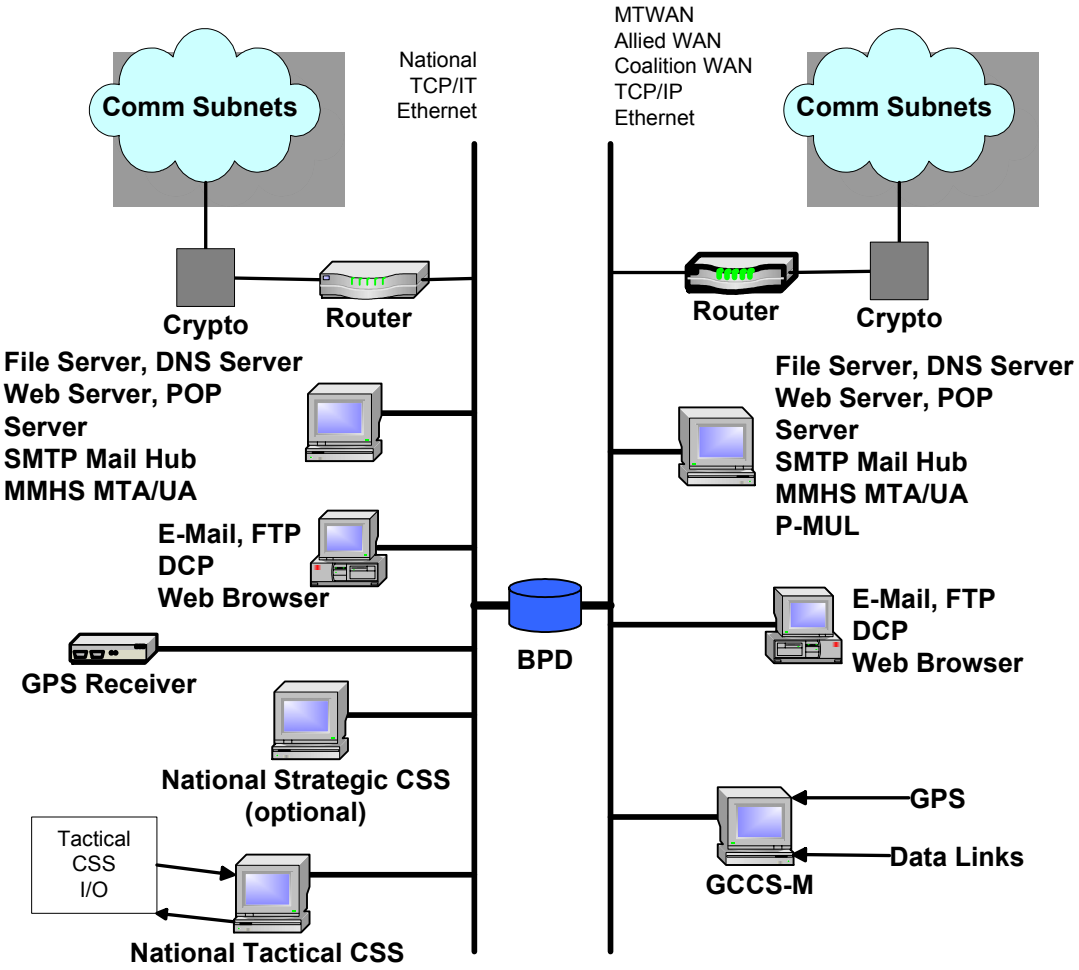

Figure 5-5: - Networked Architecture

e. A screened subnet architecture employing both network and application layer firewalls, as shown in Figure 5-6, offers a very high level of protection for the LAN from users on a remote network.

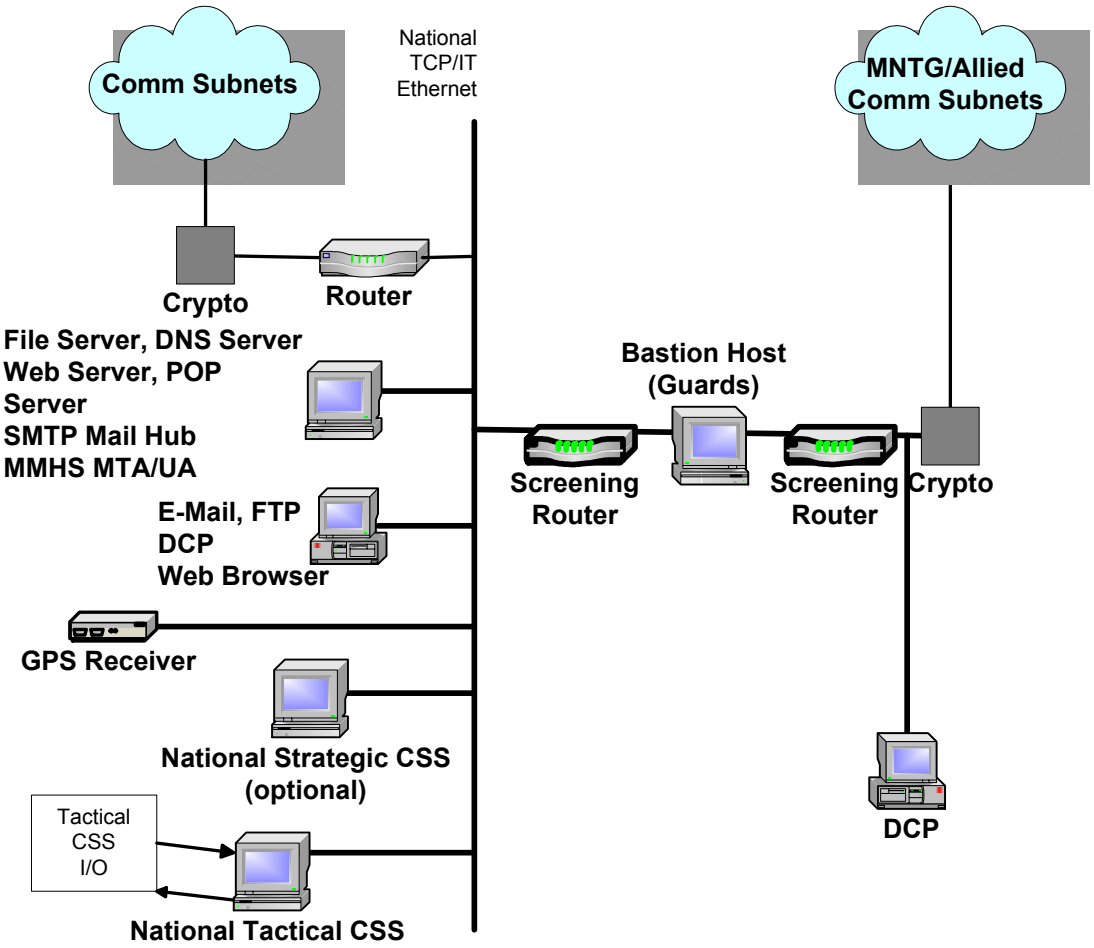

Figure 5-6: - "Fully Integrated" Target Architecture

f. The bastion host controls and audits all information flowing between the National networks and a MTWAN. It can provide proxy services to users for certain applications (e.g. FTP). The application layer proxy is used to implement virtual connections to application services on the local network. The host may be used to enforce strong authentication on connections from the allied to the national network.

g. The bastion host also contains application level guard functionality which will control the release of certain information by checking markings and content and, where necessary, by modification to meet sanitization requirements. It should be noted that particular implementations may require the guard functions to be located in machines physically separate from, but connected to, the bastion host.

h. Servers directly accessible to the Allied network will be housed in the screened subnet created between two-network layer screening routers.

i. The outer router will only permit remote users or services to access servers and application gateway on the screened subnet. Also, the outer router will only pass traffic originating from the screened subnet.

j. For incoming traffic, the inside router will be configured to accept only traffic originating from the screened subnet. For outgoing traffic, the inside router will permit access only to the screened subnet.

k. **Virtual Private Network (VPN).** VPNs, operating with approved cryptographic devices, provide network security for interoperable communications between nodes and dynamically controllable membership within private security domains (or layers).

511 ACCREDITATION

A lead nation will sponsor accreditation of a MTWAN through the Multinational Security Accreditation Board (MSAB).

512 SECURITY DEVICE INTEROPERABILITY

Operational configuration of interoperable cryptographic devices, e.g. KIV-7/KG84/BID1650 may be found in ACP 176 NATO SUPP 1.

This page intentionally blank.